Composite Signature Based Watermarking for Fingerprint Authentication

Farid Ahmed & Ira S. Moskowitz

ACM Multimedia and Security Workshop, NY, NY August 1-2, 2005

This on-line version of the paper (9 August 2005) corrects a typo in Eq. 3 from the paper that appears in the proceedings

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2005**	2. REPORT TYPE	3. DATES COVERED **00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE
Composite Signature Based Watermarking for Fingerprint Authentication

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Research Laboratory,Center for High Assurance Computer Systems,4555 Overlook Avenue, SW,Washington,DC,20375

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**7**	

Composite Signature Based Watermarking for Fingerprint Authentication

Farid Ahmed
Department of EECS
The Catholic University of America
Washington, DC 20064, USA
1-202-319-5019
ahmed@cua.edu

Ira S. Moskowitz
Center for High Assurance Computer Systems
Naval Research Laboratory
Washington, DC 20375
moskowitz@itd.nrl.navy.mil

ABSTRACT

Digital watermarking is a technology to hide information in digital media. We extend the digital watermarking technique Phasemark™, originally developed solely for image authentication, to biometrics to assist in forensic analysis. Using a signature extracted from the Fourier phase of the original image, we hide an encoded signature back into the original image forming a watermarked image. The hiding occurs in the Fourier transform frequency domain. The detection process computes the Fourier transform of the watermarked images, extracts the embedded signature and then correlates it with a calculated signature. Various correlation metrics determine the identity degree of biometric authentication. We show how a composite filter can be used in conjunction with Phasemark™ for robust authentication of fingerprints.

Keywords

Phasemark™, biometric authentication, fingerprint, watermarking, composite filter, phase only filter.

1. INTRODUCTION

With the widespread infusion of digital technologies, and the proportional ease of distribution of digital contents over the internet, digital rights management (DRM) has become an issue of critical concern. The requirements of DRM often are encapsulated in three different aspects of the computer and network assurance literature [1]. These are confidentiality of communication, integrity of contents, and access control or authentication. Confidentiality and integrity of contents have traditionally being addressed by cryptographic security protocols, while access control or authenticity verification has been addressed by both cryptographic, and non-cryptographic solutions such as digital watermarking [2], as well as by biometric authentication [3,4].

Biometric authentication refers to the verification of individuals based upon their physiological and behavioral characteristics such as fingerprint, face, iris, hand geometry, keystroke, voice, and retina identification [5-6]. Although, the acceptance and use of biometric authentication has had a slow go of it, biometric technology presently is close to maturity and is increasingly being accepted as a tool for identification and authentication [3]. Fingerprint biometrics specifically has been shown to have high effectiveness in terms of distinctiveness, permanence, and performance [6]. This is the first motivation for our paper. In particular, we show how modifications and improvements of our novel semi-robust watermarking technique Phasemark™ [7] can be used as a biometric tool for fingerprint authentication. Note, a strength of our method is that it is a *self-authentication* method, and the authentication information is carried as an integral part of the fingerprint image. Other methods may use meta-data, or an external database of fingerprint signatures to perform the authentication. In this short paper we do not do a comparison with other methods.

A motivation for the use of watermarks in biometric systems has been the need to provide increased security to the biometrics themselves and to this end, there have been some accomplishments, *e.g.*, [5-6, 8-9]. We propose to use a composite signature based watermarking technique, based upon our previous work Phasemark™, for robust fingerprint authentication, when dealing with variants of the same fingerprint. In particular, to make the authentication robust to the natural variations of different impressions of the same fingerprint, we use the notion of a training based composite filter [10-11].

2. SIGNATURE-BASED WATERMARK

2.1 Phasemark™

Let h represent a grayscale image that we wish to watermark. All processing starts on h after it has been realized in the spatial domain. We only consider compressionless TIFF, so no information is lost when going from the TIFF file format to the spatial representation as an eight bit grayscale image and back

MM & Sec '05, August 1–2, 2005, NY, NY, USA.

again to the TIFF file format (unless the image has been modified in some other manner). Note that our results are not limited to TIFF, any uncompressed image format will work, however for simplicity we use the term TIFF in this paper.

Phasemark™ was first described in [7]. Phasemark™ is a semi-robust Fourier domain authentication watermark for images. Phasemark™ has been shown to be robust to various image formats [7] and has been modified to work in the wavelet domain [15]. We use the initial Fourier domain approach in this paper. As stated, for the sake of simplicity in this paper we use a grayscale TIFF image *h*. To signify the spatial coordinates of *h* we will write *h(m,n)*. The watermark of *h* is formed from a signature of the image, taken in the Fourier frequency domain. To be specific we apply the discrete Fourier transform (DFT) to *h* and get *H*. That is $H(u,v) = X(u,v)\exp(j\phi(u,v))$, where the complex number *H(u,v)* is the *(u,v)*-th (Fourier) frequency, *X(u,v)* is the (Fourier) magnitude $|H(u,v)|$, j is the principal square root of -1, and $\phi(u,v)$ is the phase of *H(u,v)* (values are in $(-\pi,\pi\,]$). The real valued *X(u,v)* is rounded to the nearest integer and expressed as *R(u,v)*. The rounded values *R* can be expressed in bit slice format as $R=R_{q-1}, R_{q-2}, \dots , R_1, R_0$, where R_i is the i^{th} bit-plane of the rounded magnitude. We pick a specific value of *i* and modify R_i . Before we modify R_i we apply a filter *b(u,v)* to *H(u,v)* as follows:

[1]

$$\begin{aligned} b(u,v) &= +1, \text{if } \cos(\phi(u,v)) \geq 0 \\ &= -1, \text{otherwise} \end{aligned}$$

This has the effect of clamping the phase angles at either 0 or π radians. We filter the phase angles one more time by mapping the *b(u,v)* values +1(-1) to +1(0), respectively. This forms the binary phase only filter (BPOF) *B(u,v)*, which is the signature that we hide in the original cover image *h*. Using a non-avalanche (small processing errors do not grossly affect the correlation) type cipher we encrypt *B*(*u*,*v*) (symmetric key) resulting a bit plane E(*B*(*u*,*v*)). We replace R_i with E(*B*(*u*,*v*)), which results in a modified Fourier magnitude *X*(*u*,*v*)'. We apply the inverse discrete Fourier transform (IDFT) to $X(u,v)'\exp(j\phi(u,v))$, which results in our modified image *h*'. We save this file as an (uncompressed) TIFF file. We freely interchange spatial realization and the TIFF file in this paper. *h*' is the watermarked image. We note that changing the magnitude of a complex number does not change its phase angle. Therefore, the only difference between the phases of *h* and the phases of *h'* come about from the rounding done to the spatial pixel values (by clipping and clamping), not to the bit plane replacement. We use Phasemark™ for two detection correlation tests. In both tests, we assume that the detector has knowledge of the symmetric watermarking key. Before we discuss these two tests we discuss how Phasemark™ is used to determine if an image is watermarked according to the Phasemark™ algorithm (we say that such an image is *Phasemarked*), we call this the *basic correlation test.*

The basic correlation test is developed in [7]. Given a test image *t*, we determine if *t* is Phasemarked. Apply the DFT to *t*, DFT(*t*) = *T*. We extract R_i from *T* as above. We apply the decryption algorithm using the symmetric key, extract the hidden phase signature from *T*, if *T* is in fact watermarked. If *T* is not watermarked, then this extraction process should not give us the hidden signature, it gives us garbage. We verify this by a correlation test. We denote the candidate extracted signature (binary phase only filter) [13] information as *B'*(*u*,*v*). To perform the correlation test we map *B'* to {1,-1} by sending +1(0) to +1(-1). We denote this renormalized candidate hidden phase information as *b'*. We apply a phase only filter to the frequency representation of our test image *T.* That is since

[2]

$$T(u,v) = |T(u,v)|\exp(j\phi_T(u,v))$$

we use phase only filter $T_{POF}(u,v) = \exp(-j\phi_T(u,v))$. This results in values on unit circle the complex plane. These values are gauged against the candidate hidden signature *b'* (see [7] for details) by term by term multiplication. We then apply the IDFT to this matrix which results in our correlation values. The basic correlation test is not used in this paper; since our concern is not if an image is Phasemarked, rather our concern is does our fingerprint signature match what the image is telling us.

2.2 Composite Signature

The first test we perform is the *signature-authentication test.* In this, we have a generic signature, which may or may not be derived from the BPOF of the image *C* in question. However, this signature is put into *C* via the Phasemark™ method of replacing the *i*-th bit plane of the Fourier magnitude with the encrypted version of the signature. The resultant image is *C*'. Now we run the Phasemark™ correlation detector just as in the basic correlation test. That is, we extract the signature from *C*' and correlate it against the pof from *C*'. Of course, if the signature is the BPOF of C' then we are in the identical situation as in the basic correlation test. However, in the signature-authentication test we allow for more general types of signatures that enable us to "hide" more than simply the BPOF of an image back in itself. In particular, in this paper we hide a composition of BPOFs. That is, given a training set of images T_i, we have the Fourier phase $\phi_i(u,v)$ of each image. We then compute $b_i(u,v)$ of each image as before (Eq. (1)). From this we use a *majority rule algorithm* [14] and define the *composite signature* at frequency *(u,v)* by

[3]

$$\begin{aligned} B_{comp}(u,v) &= +1, \text{if} \sum b_i(u,v) \geq 0 \\ &= 0, \text{otherwise} \end{aligned}$$

The second test we perform using Phasemark™ is the *marked/unmarked test*. In this test, we take a known marked image A and compare it to an unmarked image C. If C and A are "similar" this test should result in high correlation values. In detail, we extract the hidden signature from A using the watermarking key and correlate it against the pof from C.

Therefore, we see that Phasemark™ can be generalized by using composite signatures and different correlation tests.

3. SIMULATION

3.1 Experiment Data: Fingerprints

We used the fingerprints made available at the obtained from the 'Fingerprint Verification Competition' (FVC) website [12]. We concentrated our efforts on DB3, which is generated by Amtel's FCD4B14CB FingerChip thermal sweeping sensor resulting in 80 512 dpi 300x480 images. DB3 is made up of eight different variations of 10 fingerprints. Each image in DB3 is denoted as 101_1, 101_2, 101_3, 101_4, 101_5, 101_6, 101_7, 101_8, 102_1, … , 110_8. Each image is an 8-bit gray scale image. Each image is in the TIFF format. All of the processing we do saves the image as a TIFF without compression.

As claimed in the website [12], these fingerprint impressions are markedly difficult, due to 'perturbations deliberately introduced and no efforts were made to control image quality and the sensor platens were not systematically cleaned'. The dataset was made from four fingers of each of the 30 participants. Each finger impression was taken at three different sessions, approximately two weeks apart. During the second session, individuals were requested to exaggerate skin distortion and rotation of the finger; during the third session, fingers were dried and moistened. At the end of the data collection, for each database a total of 120 fingers and 12 impressions per finger (1440 impressions) were gathered. The partial set having 10 fingers with eight different impressions is used in this simulation, which, is publicly available.

3.2 Experiments & Results

We performed seven different tests on the 80 fingerprints in DB3. We apply Phasemark™ to the images in DB3 using bit plane i=12. In the detection, the extracted signature is correlated with the computed POF of either the watermarked image (Tests 1 and 2) or the unmarked image (Tests 3-7). This results in three different classes of correlation values in tests 1-4. If the target image (marked or unmarked) is one of the training images from which the signature was computed, we call it self-correlation. If the target image is not one of those, but is still a variation of the training images, we call it in-class correlation. Finally, if the target image is from a different class of fingers, we call it out-of-class correlation. Series 1 in Figures 1-4 represents this out-of-class correlation, while Series 2 represents in-class, and series 3 represents self-correlation. In all the tests and illustrations we use the PACE (Peak-to-average correlation energy) metric as defined in reference [16] as follows.

PACE is the ratio of the highest correlation peak energy (P_{max}) to that of the average correlation energy (μ). This is a measure of sharpness of the peak and of course a high PACE value implies good correlation. We calculate this ratio in db by expressing it as

$$PACE = 20\log_{10}(\frac{P_{\max}}{\mu}) \qquad [4]$$

TESTS:

1. We obtain the usual BPOF signature from 101_1. This signature is embedded via Phasemark™ in all 80 images 101_1 to 110_8, resulting in watermarked images 101_1' to 110_8'. We perform a signature-authentication test on each image 10I_J'. The results are shown in Figure 1. The x-axis represents the fingerprint number, while the y-axis detection value in terms of PACE. Because the signature is obtained from only one impressions of a class, the in-class correlations are not as good as the self correlation, while they are slightly better than the out-of-class correlations. Note that we also did the same test nine more times, obtaining the signature from 102_1, 103_1, …, 110_1. The results were statistically indistinct from those of using 101_1. (Thus, we only illustrate 80 of the 800 results.)

2. We obtain a composite signature from 101_1,…, 101_8 using the majority rule algorithm (Eq. 3). This composite signature is embedded via into all 80 fingerprint images. Each of these 80 marked images was then run through the signature-authentication test. The results are illustrated in Figure 2 (as in Test 1 we did this nine more times for the sets 10I_1,…, 10I_8 and the results are statistically insignificant. Thus, we only illustrate 80 of the 800 results.) Note that the in-class correlation values are significantly ramped up because they were used in the signature computation.

3. We obtain a signature from 101_1 and embed that signature back into 101_1 forming 101_1'. We run the marked/unmarked test on 101_1' against all 80 unmarked images. The results are shown in Figure 3. This test is done 79 more times using the remaining 10I_J as the fingerprint to derive the signature from. The results are statistically identical to those of 101_1. (Thus, we only illustrate 80 of the 6400 results.) The results are essentially the same as in Figure 1, except that the correlation is done on the unmarked image

4. We form a composite signature (Eq. 3) from 101_1,…, 101_8. This composite signature is then embedded only in the first group of eight forming 101_1',…, 101_8'. We run the marked/unmarked test 640 times by using 101_J' against all 80 unmarked. We show the results in Fig. 4 of running the detector with 101_1' against all 80 10I_J. This is done nine more times for each of the remaining nine sets of eight versions, for a total of 6400 tests. Again, nothing is lost by only illustrating the first 80 tests. (Thus, we only illustrate 80 of the 6400 results.). Note that as in Figure 2, the in-class correlation is also as good as the self-correlation, which is very useful in distortion-invariant authentication.

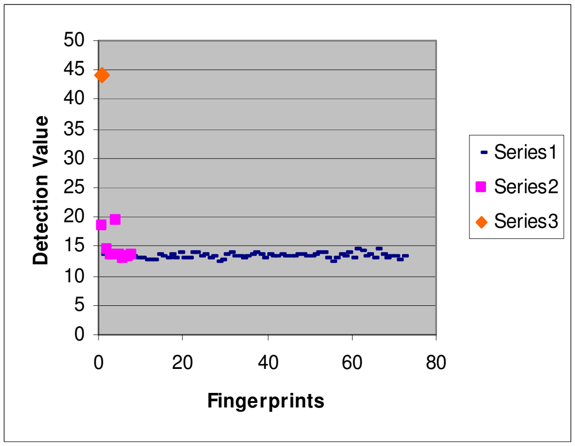

Figure 1. Distribution of Detection values from test 1

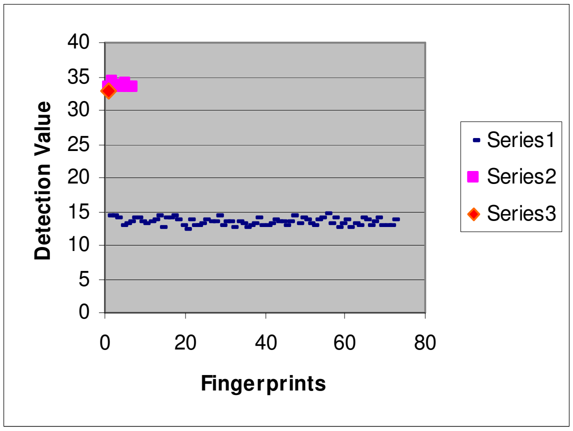

Figure 2. Distribution of Detection values from test 2

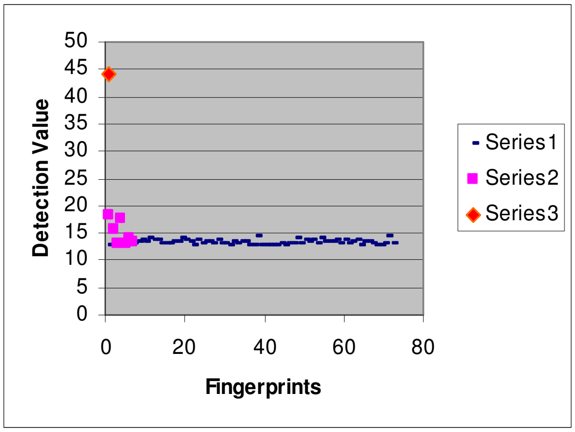

Figure 3. Distribution of Detection values from test 3

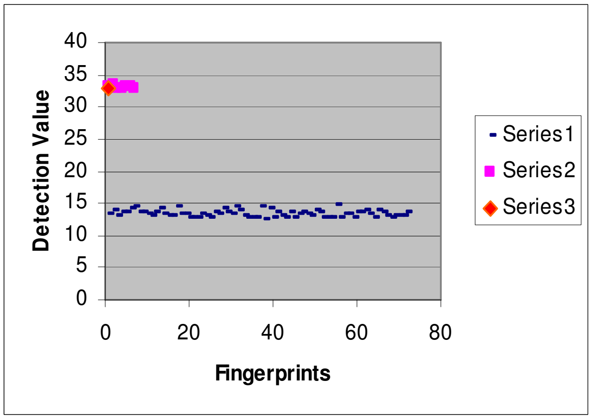

Figure 4. Distribution of Detection values from test 4

Table 1. Comparison of the first four tests

Test1 Single	Test2 Compo 8	Test3 Single	Test4 Compo 8
44.2	33	44.2	33
18.6	33.3	18.2	33.3
14.5	34.3	15.6	33.4
13.6	33.7	13	33
19.4	33.5	17.8	32.9
13.5	34	13	33.2
13.1	33.5	14	33.3
13.2	33.3	13.5	33
13.5	14.4	12.8	13.4
13.1	14.4	13.4	13.8
13.6	13.9	13.3	13.1
13.4	12.9	12.6	13.5
13.5	13.2	12.7	13.6
14	13.5	13	14.3
14	14	13.2	14.6
13.4	13.9	13.4	13.6

Table 1 summarizes the PACE results from first 4 tests. The first eight entries in each column are the correlation statistics for a fingerprint and its seven variants (which was used in the signature computation for tests 2 and 4). The next eight entries in each column are the correlation statistics coming from eight variants of a non-trained finger.

5. This is similar to Test 4, except that the composite signature is formed from 101_1 and 101_2 and we

embed the composite signature into the first group of eight forming 101_1',…, 101_8'.

6. This is similar to Test 4, except that the composite signature is formed from 101_1, 101_2, 101_3, and 101_4. and we embed the composite signature into the first group of eight forming 101_1',…, 101_8'.

7. This is similar to Test 4, except that the composite signature is formed from 101_1, 101_2, 101_3, 101_4, 101_5 and 101_6. and we embed the composite signature into the first group of eight forming 101_1',…, 101_8'.

Note that tests 5-7 are variations of test 4, where they differ in the number of fingerprint impressions used in computing the composite signature. Therefore, we are not displaying the partial correlation distribution as in Figure 4. Instead, Table 2 enumerates the difference in (PACE) detection performance. For example, Test 5 uses the first two impressions and consequently correlation statistics for these two are significantly higher than all others. Similar observation can be made for Test 6 and 7 results (column 3 and 4 from Table 2).

Table 2. Detection performance with different composite signature

Test4 Compo 8	Test5 Compo 2	Test6 Compo 4	Test7 Compo 6
33	39.1	36.4	34.5
33.3	39	36.4	34.9
33.4	13.6	36.1	34.5
33	13.2	36.2	34.5
32.9	14.3	13	34.4
33.2	13.7	13.6	34.6
33.3	13.4	13.4	12.9
33	15.4	13.3	13.2
13.4	14.7	13.8	13.5
13.8	14.1	12.8	12.7
13.1	14.2	13.8	13.4
13.5	13.8	13.3	13.2
13.6	13.2	13.5	13
14.3	13.1	13.2	12.8
14.6	13.4	12.9	13
13.6	14.2	13.9	15.7

Let us now see closely the contribution of composite signature in this authentication scheme. Here we focus on the two tests done in test 3 (without composite signature) and 4 (with composite signature). Figure 5 and 6 show the PACE value distribution of all 6400 correlation tests done in tests 3 and 4 respectively. Figure 5 demonstrates the histogram of correlation values, when no composite signature is used. Note that there is even overlap of correlation values coming out of forged and authentic fingerprints. By forged, we mean that the fingerprint was not part of the signature generation process. Of course a fingerprint is considered authentic if it used to form the signature (composite or non-composite). Figure 6 shows the corresponding results with the composite signature. The separation between the distributions for forged and authentic is now very clear. This can be used to choose a threshold for fingerprint authentication, as demonstrated by Figure 7 Receiver Operating Characteristics (ROC). Note AAR is authentic acceptance ratio, and FAR is false acceptance ratio (see [9]).

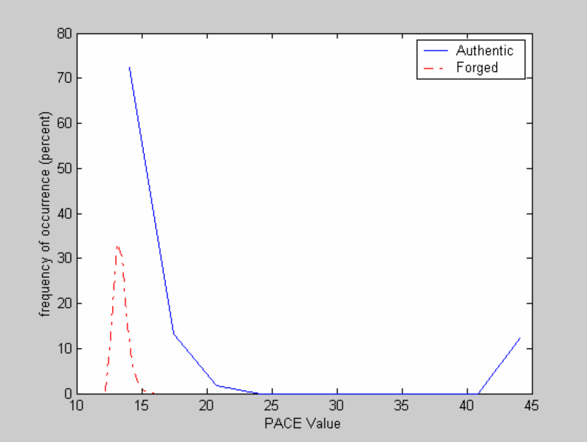

Figure 5. Histogram of detection metric with no composite signature (Test 3)

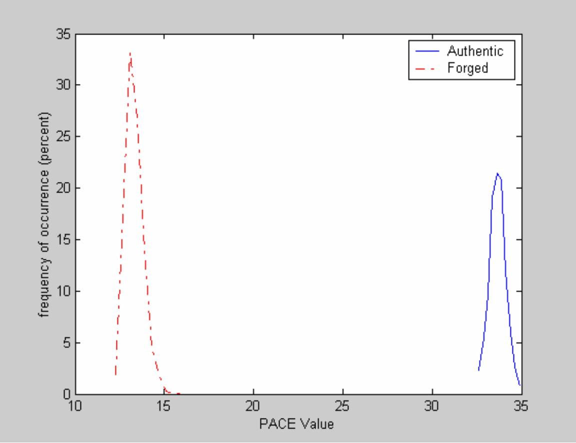

Figure 6. Histogram of detection metric with composite signature (Test 4)

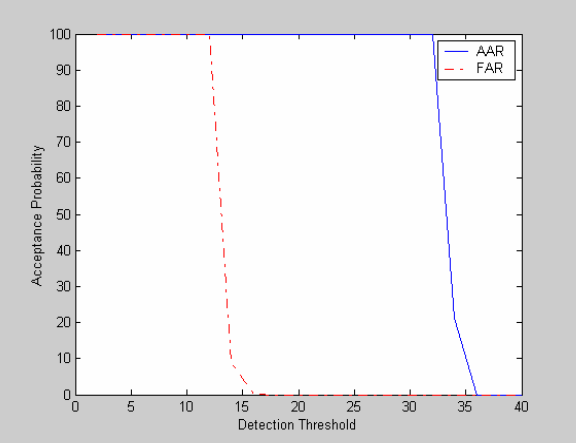

Figure 7. Receiver Operating Characteristics with composite signature (Test 4)

4. CONCLUSIONS

In this work, we have extended Phasemark™ [7] to the important application of fingerprint authentication. We demonstrate two different scenarios of applications, where the original image may be present or absent. We demonstrate the usefulness of having a composite signature obtained from distorted versions of fingerprint impressions. The composite filter based solution results in robust authentication performance. Further work need to be done to make it more robust so that it will work well with non-trained fingerprints as well.

5. ACKNOWLEDGMENTS

Our thanks to Office of Naval Research. We thank the reviewers for their help comments.

6. REFERENCES

[1] William Stallings, Cryptography and Network Security-Principles and Practices, 3rd ed. Prentice Hall, 2003.

[2] Ingemar Cox, Jeffrey Bloom, Matthew Miller, *Digital Watermarking: Principles & Practice*, 2001, Morgan Kauffman Publishers, ISBN 1-55860-714-5, ch. 1-2.

[3] A. K. Jain, A. Ross and S. Prabhakar, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics*, Vol. 14, No. 1, pp. 4-20, January 2004.

[4] A.K. Jain, L. Hong, S. Pankanti, and R. Bolle, “An identity-authentication system using fingerprints,” Proc. of the IEEE, vol. 85, no. 9, 1365-1388, 1997.

[5] Claus Vielhauer and Ralf Steinmetz, “Approaches to Biometric watermarks for owner authentification,” Proc. SPIE, vol. 4314, pp. 645-651.

[6] U. Uludag, Sharath Pankanti, S. Prabhakar, and A. K. Jain, “Biometric Cryptosystems issues and Challenges,” Proc. IEEE, vol. 92, no. 6, pp. 948-960, 2004.

[7] Farid Ahmed and Ira S. Moskowitz, “A Correlation-based Watermarking Method for Image Authentication Applications,” Optical Engineering Journal, Aug 2004.

[8] B. Gunsel, U. Uludag, and A. M. Tekalp, “Robust Watermarking of Fingerprint Images,” Pattern Recognition, vol. 35, no. 12, pp. 2739-2747, Dec 2002.

[9] A. K. Jain, Umut Uludag, “Hiding Biometric Data,” IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 25, no. 11, pp. 1494-1498, 2003.

[10] B.V.K. Vijayakumar, Marios Savvides, C. Xie, K. Venkatramani, and J. Thornton, “Using Composite Correlation Filters for Biometric Verification,” Proc. SPIE, Vol. 5106, pp. 13-21, 2003.

[11] Farid Ahmed and M. A. Karim, “Binarized composite filter design using majority-granted nonlinearity,” *Computers and Electrical Engineering,* Vol. 23, No. 5, pp.283-299 (1998).

[12] Fingerprint Verification Competition http://bias.csr.unibo.it/fvc2004/download.asp FVC Fingerprint database.

[13] J. L. Horner and J. R. Leger, “Pattern Recognition with Binary phase-only filters,” *Appl. Opt*., vol. 24, pp. 609-611, 1985.

[14] Farid Ahmed and M. A. Karim, “A Filter-feature-based Rotation Invariant Joint Fourier Transform Correlator,” *Applied Optics*, Vol. 34, No. 32, pp. 7556-7560 (1995).

[15] Farid Ahmed and Ira S. Moskowitz, “Phase Signature-based Image Authentication Watermark Robust to Compression and Coding,” Mathematics of Data/Image Coding, Compression, and Encryption VII, with Applications, ed. M.S. Schmalz, Proc. Of SPIE Vol. 5561, pp. 133-144, Denver, 2004.

[16] B.V.K. Vijay Kumar and L. Hassebrook, “Performance Measures for Correlation Filters,” *App Opt*, Vol. 29, no. 20, pp. 2997-3006.